

Legyen óvatos!

Már magyar nyelven is terjednek Sextortion zsarolólevelek, mutatjuk mire érdemes figyelni!

Feladó: Névtelen Hacker (sheri.787@h.nevtelenhacker.top)
Címzett: Te@email.hu

Árulkodó a feladó e-mail címe:

timothy.916@b.nevtelenhacker.top

Mindig nézzük meg a feladó címet, mert néhány esetben a küldő címéből is megállapítható a levél gyanús tartalma.

Tárgy: Ez az utolsó figyelmeztetésem

Sürgető hangnem, helyesírási hiba

üzenet

UTOLSÓ FIGYELMEZTETÉS

Fontos, hogy ne essen pánikba!

Olvassa át többször a levelet, hogy kiszűrje a gyanús elemeket.

Önnek lehetősége van arra, hogy megmentsse a társadalmi életét - nem vagyok viccelő!

Az utolsó 72 órát adom meg a fizetés előtt, mielőtt elküldöm a videóit maszturbációval az összes barátodnak és társának.

Amikor utoljára látogattál egy fiatal tinédzserként egy Pornográf weboldala, letöltötted és automatikusan telepítetted a létrehozott kémsoftvert.

A program bekapcsolta a fényképezőgépet, és rögzítette a maszturbációját és a nézett videót maszturbálás közben.

Szoftverem szintén letöltött e-mailek listáját és a Facebook-ismerőseinek listáját a készüléken.

Mind a - Cert.mp4 - mind a maszturbációval és egy fájlt a merevlemezemen található összes kapcsolattal.

Rejtett speciális karakterek, hogy a levél ne akadjon meg a spamszűrőn

Nagyon **D**arverz!

Ha azt szeretné, hogy mindkét fájlt töröljem és titokban tartsam, akkor **elküldned kell nekem** a Bitcoin fizetést.

Utolsó 72 órát adok át a pénzeszközök átutalására.

Furcsa nyelvezet, helyesírási hibák

Ha nem tudja, hogyan kell fizetni a Bitcoinnal, látogasson el a Google-ra és keressen - hogyan vásároljon bitcoint.

Közvetlenül küldjön 500.000 HUF (0.342384 BTC) erre a Bitcoin címre:

Soha NE fizesse ki a kért összeget!

Semmi nem garantálja, hogy a zsaroló tényleg rendelkezik Önről információkkal.

38tP8HBP eEqKuHEoH3uxWG3Nenz5rUxsRi
(másolja és illessze be)

1 BTC = 1.493.500 HUF most, így pontosan 0.342384 BTC küld a fenti címre.

Folyamatosan változtatják a közvetlen és közvetett (tegezés/magázás) megszólításokat.

Ne próbálja meg csalni!

Amint megnyitja ezt az e-mailt, tudom, hogy kinyitotta.

Ez a Bitcoin cím csak Önhöz kapcsolódik, így tudni fogom, hogy elküldte a megfelelő összeget.

Teljes fizetés esetén mindkét fájlt eltávolítjuk, és kikapcsolom a szoftvert.

Ha nem **küldi el** a fizetést, elküldöm a maszturbációs **videókat** az összes ismerősének és társának, amelyet a letöltött kapcsolattartó listáról küld.

Íme a fizetési részletek:

Amennyiben ilyen, vagy ehhez hasonló üzenetet kap egyszerűen törölje a levelet.

Küldj 0.342384 BTC erre a Bitcoin címre:

38tP8HBP eEqKuHEoH3uxWG3Nenz5rUxsRi

(másolja és illessze be)

Meglátogathatja a rendőrséget, de senki sem segít.

Tudom, mit csinálók.

Nem élek az Ön országában, és tudom, hogy maradjon névtelen.

Ha mégis felmerül annak gyanúja, hogy a zsaroló valós információkkal rendelkezhet Önről, tegyen feljelentést az illetékes hatóságnál, illetve továbbítsa levelét mellékletként (fejléccel együtt) a **cert@nki.gov.hu** e-mail címre.

Ne próbáljon meg becsapni - azonnal tudni fogom - az én Spysoftom rögzíti az összes meglátogatott weboldalt és az összes nyomógombot.

Ha ezt teszed - elküldöm ezt a csúnya felvételt mindenkinek, akit ismersz, beleértve a családot is!

Ne csalsz meg! Ne felejtse el a szégyenet, és ha figyelmen kívül hagyod ezt az üzenetet, az életed tönkremegy.

Várom a Bitcoin fizetését.

Névtelen Hacker

Ui Ha több időre van szüksége a BTC vásárlásához és elküldéséhez, nyissa meg a jegyzetombót, és írjon be - 48H ++ - és mentse el. Így kapcsolatba léphet velem.

Még 48 órát fogok adni, mielőtt elküldöm a videókat a kapcsolattartóknak, de csak akkor, ha látom, hogy valóban meg akarod vásárolni bitcoint.

Névtelenek vagyunk.

Nem megbocsátunk. Nem felejtjük el.

Elvárájuk tőlünk.

A Sextortion zsarolólevelek egy másik - jellemzően külföldi - verziójában a felhasználók korábban kiszivárgott online bejelentkezési adatait is feltüntetik. A támadók ezzel próbálják meg állításukat - hamisan - hitelesebbé tenni.

Ilyenkor sem szabad megijedni!

- Ellenőrizze e-mail címeinek és jelszavainak lehetséges kompromittálódását (haveibeenpwned.com).

- Rendszeresen változtassa meg jelszavait: javasolt a hosszú és összetett jelszavak használata, amely kis- nagybetűt, számot és speciális karaktert is tartalmaz.

- Eltérő szolgáltatásokhoz, eltérő jelszavakat alkalmazzon, amennyiben van rá lehetőség engedélyezze a kétfaktoros azonosítást.